# Information Security Risk Assessment: A Method Comparison

Gaute Wangen,
CCIS,
NTNU Gjovik
Teknologiveien 22, 2802 Gjovik, Norway
Email: gaute.wangen@ntnu.no

***Abstract*—Information security risk assessments (ISRA) are per-formed daily according to different standards and industry methodologies, but how does the choice of a method affect the assessment process and its end results? This research qualitatively investigates the observable differences in effects from choosing one method over another. Through multiple empirical case studies, our work compares the application of three ISRA methods. We first outline the theoretical differences between the three methods and then analyze the experience data collected from the risk assessment teams. Finally, we examine the metadata of the produced risk assessments to identify differences. Our study found that the choice of a method influences the assessment process, along with its outcome.**

***Keywords*—Information Security, Risk Assessment, Case study.**

*Information Security Risk Assessment: A Method Comparison. IEEE Computer Magazine Special Issue: Cyber Physical Systems and Security Risk Assessment, 2017, 50(4), 52-61.* [1]

## I. INTRODUCTION

Currently, there are numerous information security (InfoSec) risk assessment (ISRA) methods to choose from [1], but scarce information on how to choose and if this choice matter for the result. Since multiple ISRA approaches exist, it is in the interest of the InfoSec community if this choice matters for the outcome, both for improving decision basis, increasing security levels and maximizing return on investment. This paper compares three different ISRA methods; *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Allegro)* (OA) [2] and *ISO/IEC 27005:2011 - Information Security Risk Management* (ISO27005) [3], together with one Norwegian method; *Norwegian National Security Authority (NSM) Guidelines in Risk and Vulnerability Assessments (NSMROS)* [4]. This study considers three types of empirical comparisons; comparison through practice, method content, and the produced results from application. The data for this study was collected through multiple risk assessment case studies in a Norwegian academic institution. Firstly, we apply the results from Core Unified Risk Framework (CURF) [5] to define distinctiveness of each method. Secondly, we collect and analyze experience data from ISRA groups. Finally, we apply CURF in a novel way to compare ISRA metadata results. While numerous studies of ISRA methods exist [1], [6], [7], this is the first study that we are aware of in which the methods are practically applied and compared. The main benefit of this paper is new knowledge regarding ISRA method performance, both in the results and experiences with the methods, in addition to our proposed comparison method establishing cause-effect relationships. The scope of this study is limited to risk assessment and treatment as defined in the ISO 27000-standards [8], [3].

The following section describes the necessary background information and terminology used in this paper for the reader to be able to follow. The related work primarily contains a presentation of CURF and differences between the three ISRA methods. Furthermore, we present the research method, which describes the case studies, empirical data collection, and analysis of both experience data and ISRA results. Finally, we present the results and analysis of the experience data and the ISRA reports using CURF, before discussing the results and concluding the paper.

## II. BACKGROUND AND RELATED WORK

This section presents a summary of the fundamental concepts for understanding the ISRA discipline and the terminology applied to the remainder of this article. In addition, we introduce the previous work that has motivated this study, in particular, CURF and the included ISRA methods.

### A. Information security risk assessments

InfoSec risk comes from applying technology to information [9] and the primary goal of InfoSec is to secure the business against threats and ensure success in daily operations by ensuring confidentiality, integrity, availability, and non-repudiation [8]. Best practice InfoSec is highly dependent on well-functioning ISRM processes [9] which is the practice of continuously identifying, reviewing, treating and monitoring risks to achieve risk acceptance [3]. Risks for information systems are defined as an adverse event with estimations of consequence (C) for the organization (e.g. financial loss) and the corresponding probability (P) of the event occurring. Further, the ISRA results are assessed by the decision-maker, and if found unacceptable, steps are taken to mitigate the risk to the organization. A *risk assessment* consists of the

[1] The forthcoming version in IEEE Computer Magazine has been edited to fit the style and requirements of the publication channel.

overall process of risk analysis and risk evaluation [8], and *risk analysis* is the *systematic use of information to identify sources to estimate the risk*[8]. Risk evaluation is the *process of comparing the estimated risk against given risk criteria to determine the significance of the risk* [8], while risk treatment represents the chosen strategy to address an unacceptable risk.

### *B. CURF and included ISRA Methods*

Several frameworks exist for theoretically comparing ISRM/RA methods with each other (e.g. [1], [6]). However, the existing approaches are primarily scoped to evaluate ISRA content to a predetermined set of criteria, which is equivalent to a top-down approach and quite restrictive as differences not present in the criteria will be overlooked. This scheme makes them less suited for analyzing cause-effect relationships between method and results, since causes not present in the criteria may be neglected. The CURF bottom-up approach [5] solves this problem by mapping ISRA method content and using it as comparison criteria. For each added method reviewed in CURF, we identify which tasks the approach covers and combine all the tasks covered by all surveyed methods into a combined set. The evaluation of the ISRA method consists of investigating to what extent the said method covers all undertakings present in the already created superset. This approach makes CURF a bottom-up comprehensive comparison where the criteria are determined by the method tasks rather than being pre-determined. The included ISRA approaches are functional and formal ISRA methods that focus on assessments of assets, threats, and protections, often with measures of P and C [10]. CURF has three scores for each identified task: *Addressed* when a task is fully addressed with clear descriptions on how to solve it, *Partially addressed* when an undertaking is mentioned but not substantiated, and *Not addressed* for methods that do not mention or address a particular task at all. CURF provides a measure of completeness for the studied methods, see bottom row in Table I.
Table I highlights how the approaches differ, where the summary of each column shows completeness. The row scores reveal how well the ISRA methods scored overall. The three ISRA methods included in this study was also used as input for developing CURF (see [5]), following is a summary of each method and their differences.

*1) NSMROS:* The Norwegian NSMROS [4] was derived from the Norwegian Security Act for compliance purposes. We initially applied NSMROS because our teams were Norwegian and the method had a good standing in the Norwegian ISRA community. NSMROS is a sequential [10] probabilistic approach centered on assets protection, threat, and vulnerability, and provides few activities outside of this.

*2) OCTAVE Allegro (OA):* is a lightweight version of the original OCTAVE and was designed as a streamlined process to facilitate risk assessments, and reduce the need for InfoSec experts while still producing robust results [2]. OA was recommended to us by several experts in the field as an established method with several academic citations and references. OA is a checklist approach (*assistant*[10]) due to the amount of worksheets it provides to the practitioner. In OA a risk is an event with corresponding consequence and uncertainty. Instead of probability, OA instead focuses on subjective estimates of consequence in the form of impact areas.

TABLE I. CURF, MAIN QUALITATIVE DIFFERENCES BETWEEN FRAMEWORKS

| | NSMROS | OCTAVE A | ISO/IEC27005 | Row Sum |
|---|---|---|---|---|
| *Risk Identification* | | | | |
| Preliminary Assessment | 2 | 2 | 0 | 4 |
| Risk Criteria Determination | 1 | 2 | 2 | 5 |
| Business Objective Identification | 0 | 2 | 2 | 4 |
| Stakeholder Identification | 0 | 1 | 2 | 3 |
| Asset Identification | 2 | 2 | 2 | 6 |
| Mapping of personal data | 0 | 1 | 1 | 2 |
| Asset Evaluation | 2 | 1 | 1 | 4 |
| Asset Owner & Custodian | 0 | 2 | 2 | 4 |
| Asset Container | 0 | 2 | 0 | 2 |
| Business Process Identification | 0 | 0 | 2 | 2 |
| Vulnerability Identification | 1 | 1 | 2 | 4 |
| Vulnerability Assessment | 0 | 0 | 2 | 2 |
| Threat Identification | 2 | 2 | 2 | 6 |
| Threat Assessment | 1 | 2 | 2 | 5 |
| Control Identification | 0 | 1 | 2 | 3 |
| Control Assessment | 0 | 0 | 2 | 2 |
| Outcome Identification | 2 | 2 | 2 | 6 |
| *RI Completeness* | 13 | 23 | 38 | |
| *Risk Estimation* | | | | |
| Threat Willingness/Motivation | 0 | 2 | 2 | 4 |
| Threat Capability (know how) | 0 | 0 | 1 | 1 |
| Threat Capacity (Resources) | 0 | 1 | 1 | 2 |
| Vulnerability Assessment | 2 | 0 | 0 | 2 |
| Qualitative Probability Est. | 1 | 1 | 2 | 4 |
| Quantitative Probability Est. | 1 | 0 | 2 | 3 |
| Quantitative Impact Estimation | 2 | 1 | 2 | 5 |
| Qualitative Impact Estimation | 2 | 2 | 2 | 6 |
| Level of risk determination | 0 | 0 | 2 | 2 |
| Risk Aggregation | 0 | 1 | 2 | 3 |
| *RA Completeness* | 8 | 8 | 16 | |
| *Risk Evaluation* | | | | |
| Risk Prioritization/Evaluation | 2 | 2 | 2 | 6 |
| Risk Treatment Recommendation | 0 | 2 | 0 | 2 |
| *RE Comp* | 2 | 4 | 2 | |
| *Completeness* | 23 | 35 | 46 | |

*2=Addressed*
*1=Partially Addressed*
*0=Not Addressed*

*3) ISO/IEC 27005:2011 - Information technology - Security techniques - Information security risk management [3]:* details the complete process of ISRM/RA, with activities, inputs, and outputs of each task. It centers on assets, threats, controls, vulnerabilities, consequences, and likelihood. The ISO27005 scored the highest on the ISRA completeness measurement [5], Table I. We chose to include the ISO/IEC 27005:2011 as it is regarded as the best practice standard for ISRM. ISO27005 is a sequential method that comes with an extensive appendix, supporting the user in scoping the assessment, and the asset, threat, and vulnerability assessments.

## III. Method

This study includes the results from four case studies conducted with each method and twelve risk assessments in total collected over five years. For the case studies, we had independent risk assessment teams running projects primarily at the strategic and tactical level at an educational institution. Each group conducted one assessment using one primary method for their project. Further, we collected and compared the experience data from the groups using interviews and questionnaires. Lastly, we applied CURF to analyze the resulting risk assessment report and to establish a cause-effect relationship between method and result. The following subsections substantiate each step in the research process.

### A. Research design

The case studies were risk assessments of real-world targets in an academic institution as a part of a mandatory ISRM course. The local IT organization provided the assignments and made available resources to assist the projects. The end reports were the primary deliverable and used in the local ISRM program for decision-making. Each case study was performed by a homogeneous group of InfoSec students, with group sizes ranging from six to ten participants. All of the participants had received basic training in InfoSec, but had no experience following formal ISRA methodologies. All groups completed a six-week basic ISRA training before conducting the primary task. The researchers participated as supervisors and subject-matter experts. All the groups followed one method, completed their risk assessment projects within four months, and presented their findings to the decision-makers. The groups primarily used interviews and online sources for data collection, supplemented with questionnaires, observations, and sampling. The experiment did not allow technical tools for active penetration testing. Each group delivered their findings in a final report, which outlined identified risks, analysis, and proposed treatments. The groups applied one ISRA method but were given access to supplementing literature which they could use as needed.

### B. Data collection and Sample

We designed a survey to collect qualitative experience data at the end of each project. Key areas of interest were experiences with applying each method, how the groups used it, together with advantages/disadvantages of the method. The survey also mapped each groups dependency on supporting literature. As for the level of measurement, the instrument had category, ordinal, open-ended, and continuous type questions. Category for demographics and categorical analysis, while the main bulk of questions were designed using open-ended and ranking questions, with the latter using the Likert scale *1 - Not at all*, *2 - Low*, *3 - Medium*, *4 - High*, and *5 - Very high*. For NSMROS and ISO27005, we ran the data collection as an online questionnaire, while we conducted face to face interviews with the OA groups. In total, this study incorporates 26 answers to questionnaires, and four group interviews including 8-10 people per interview.

### C. Qualitative Data Analysis

For *Descriptive analysis* we have considered distributions using the median together with range, minimum-maximum values, and variance. We also conducted *Univariate* analysis of individual issues, and *Bivariate* analysis for pairs of questions to see how they compare and interact. This study also analyses the distributions of the answers, for example, if they are normal, uniform, bimodal, or similar. *Crosstabulation* was applied to analyze the association between two category type questions. The survey had several open-ended questions which we have treated by listing and categorizing the responses. Further, we counted the occurrence of each theme and summarized the responses.

### D. Risk Assessment Report Analysis

Since the variety of targets for the risk assessments was too diverse to compare findings, instead we studied the focus areas and metadata. For each of the four ISRA reports produced with each method, we applied the CURF bottom up approach and mapped the contents of each report and combined them for comparison with the other methods. Each identified area, e.g. "Threat Assessment," was scored by the same system as CURF (not addressed - 0, partially - 1, and addressed - 2). Since we had four reports for each method, we qualitatively assessed each report and added the total score (maximum 8) for each method for comparison. In order to make the theoretical and risk reports results comparable, we assigned the following ranges: 0-2 equals *Not Addressed*, 3-5 equals *Partially addressed*, and 6-8 equals *Addressed*.

## IV. Experiences using the ISRA methods

This section summarizes the experiences reported by groups using NSMROS, OA, and ISO27005, presented in that order. We start with the reported advantages and disadvantages of applying each method, before discussing the method's appendices, customization, use of supporting literature, and data collection.

### A. Advantages and disadvantages of each method

Our results show that the participants were equally satisfied with their methods, all perceived as *4 - Highly Useful*, where NSMROS received the single lowest score (*2 - Low*) and ISO27005 the highest (*5 - Very high*). Our results showed that the reported difference in perceived usefulness between the ISRA methods was minimal. Table II summarizes the advantages and disadvantages from using each method.

*1) NSMROS:* was easy to understand and apply, where the two most frequently mentioned points was that the process was well explained and defined, together with being sequential and easy to follow. Besides, the method was reported to be versatile with easy-to-distribute tasks. NSMROS was also reported to be easy to use and well suited for beginners. Another advantage was that NSMROS is written in the native language which made it easier to understand.
The main disadvantages was that the how-to description of each step in the method was scarce with insufficient explanations of key tasks. There was also a lack of examples both in the text and from other sources which made the process hard to follow.

*2) OA:* had several advantages, such as being easy to follow with a systematic and comprehensive process. Regarding the latter point, the OA checklist approach created a rigorous assessment, which also forced the groups to research areas that else could have been overlooked. The focus on organizational drivers was a positive trait of the method as it forced a better organizational understanding. The groups also reported consequence estimation as one of OA's strong suits. The groups also said that OA is easy to apply once they had learned it. The overall assessment was that the worksheets and templates worked well to support their risk assessments.

On the reported disadvantages, all groups reported OA to be hard to understand and learn because it was overwhelming and the non-native technical language left more room for misunderstanding. All groups found the organizational drivers hard to define, and the time spent working on the drivers may not have been worth the effort. OA was also too rigid and dependent on the worksheets, which caused some of the groups to get stuck on tasks just producing worksheets. One example of this is that OA requires one schema per critical asset. OA is a rigid methodology and requires one task to be completed before starting the next, which hindered efficiency in the large groups and limited the opportunity for conducting parallel tasks. The groups reported that the lack of focus on probabilities made it hard to differentiate, prioritize, and communicate risk with equal consequence. All groups also reported the project to have too many participants (8-10) to apply OA.

*3) ISO27005:* main advantage was a comprehensive task, process descriptions, detailed approaches, and ISO27005 on an overall was perceived as a useful tool for ISRA. Regarding the process descriptions, the groups found the clearly described inputs and outputs of each process particularly useful. ISO27005 was reported as well structured, easy to look up and use as a point of reference. The groups also easily found existing examples of applications and checklist templates on what to include in the analysis useful. The standard was easy to apply in practice and provided a nice introduction to ISRA.

The main disadvantages with ISO27005 were that it was a challenging read and hard to grasp for novices caused by the extensive use of technical expressions, interpretations, and technical terminology. The comprehensiveness of the framework made it hard to find relevant information, learn, and understand. These issues were especially prominent when the groups were working on understanding the tasks, finding where to begin, and scoping the project. The eight groups working with ISO27005 and OA all struggled with the technical non-native language of the methods.

### B. Method Independence

All three included methods adhered to the practice of describing the primary process in the main document and then substantiate each step in the appendices. This part first analyzes the usefulness of the appendices of each method, before investigating how the groups applied supplementing literature for their assessments.

*1) Appendices and Supplementary material:* The appendices in NSMROS are primarily worksheets addressing ISRA planning, asset and system identification, and risk identification. The NSMROS groups reported a low usefulness overall for the appendices. The OA Worksheets (Appendix B) and Example Worksheets (Appendix D) covers assets, risk criteria, impact areas, and risk estimation, and were both reported as highly useful. The groups considered supplementary method guidance (Appendix A) as medium useful in the ISRA project. None of the groups made use of the questionnaire worksheet (C).

ISO27005 has five primary appendices: Annex A is intended to assist the practitioner in scoping the assessment. (B) addresses asset identification and evaluation, (C) addresses threat identification, (D) addresses vulnerability identification and assessment, and (E) provides strategies and tools for performing an ISRA. All the ISO27005 Appendices were perceived as useful. Although the median was three (medium) for all the appendices, the results show that eight or more of the respondents found Annex B and C high or very highly useful.

*2) Use of Supplementing literature:* One of the premises of the study was that the groups had access to a set of supplementing literature in a shared repository together with open sources. We asked the participants about their reliance on supporting literature for the risk assessment. All groups frequently applied the local security policy and principles document in their assessment. However, supporting literature was not frequently used overall. For the NSMROS groups, ISO27001 was most often used together with ISO27002. The OA groups primarily used supplementing literature for $PxC$ calculations and to derive organizational drivers. The ISO27005 groups reported that they sometimes used the foreign and domestic threat assessments together with native language resources. As an overall, the need for supporting literature seemed consistent and similar with all three approaches. The noticeable difference is that ISO27001 was used more frequently with the NSMROS groups. Another difference is that the OA and ISO27005 groups scored higher on native language ISRA resources. The right column in Table II summarizes the reported needs covered with supplementing literature for each approach.

TABLE II. SUMMARY OF REPORTED ADVANTAGES, DISADVANTAGES, AND NEEDS COVERED WITH SUPPORTING LITERATURE FROM EACH METHOD

| | **Advantage** | **Disadvantage** | **Supplementing Literature** |
|---|---|---|---|
| *NSMROS* | - Well defined sequential process<br>- Well explained process<br>- Nice introduction to ISRA<br>- Easy to distribute tasks<br>- Native language | - Too generic task descriptions<br>- Lack of examples<br>- Vague estimation metrics | - Templates<br>- Examples<br>- How-to ISRA<br>- Scoping |
| *OCT A* | - Adaptable<br>- Systematic and comprehensive process<br>- Worksheets<br>- Easy to use once learned | - Hard to learn and understand<br>- Probability not prioritized<br>- Too rigid | - Probability<br>- Asset evaluation<br>- Threat identification<br>- Organizational Drivers<br>- ISRA explanations in native language |
| *ISO27k5* | - Detailed descriptions<br>- Well structured<br>- Nice reference<br>- Easy to apply | - Heavy reading<br>- Hard to grasp<br>- A lot of irrelevant info for one ISRA project | - Threat assessments<br>- PxC Estimations<br>- Terminology<br>- Definitions<br>- ISRA explanations in native language |

## V. Analysis and Discussion

This section first presents the comparison of CURF and the ISRA reports. Secondly, we compare the experienced differences with CURF.

### A. Differences in the Risk Assessment Reports

Having outlined the differences in ISRA method application, this study proceeds to analyze differences in ISRA reports. We applied the CURF approach to assessing the qualitative differences in the risk assessment results and identified twenty-six documented tasks in the reports. Table III outlines the tasks and the overall qualitative differences in the content of the delivered reports; the completeness score reveals a clear difference between the methods with the ISO27005 groups scoring the highest.

TABLE III. OBSERVABLE DIFFERENCES IN THE RISK ASSESSMENT REPORTS. MAX SCORE 8 PER METHOD, 24 PER ROW, AND WITH 26 IDENTIFIED TASKS, AND 208 PER COLUMN.

| *Tasks* | *Subtasks from Report* | *Source* | NSMROS | OA | ISO | Row |
|---|---|---|---|---|---|---|
| Case Description | | | | | | |
| | Organizational Drivers | OA | 6 | 2 | 4 | 12 |
| | Risk Measurement Criteria | C | 7 | 8 | 8 | 23 |
| | Organizational Goals/ Business objectives | C | 4 | 5 | 8 | 17 |
| Risk Identification | | | | | | |
| | Stakeholder Identification | C | 8 | 8 | 8 | 16 |
| | Asset identification | C | 6 | 8 | 8 | 22 |
| | Asset evaluation/Criticality | C | 3 | 8 | 8 | 19 |
| | Asset Container | C | 0 | 7 | 3 | 10 |
| | Threat Identification | C | 4 | 8 | 8 | 20 |
| | Threat Assessment | C | 1 | 3 | 8 | 12 |
| | Areas of concern/ Vulnerability identification | C | 8 | 8 | 8 | 24 |
| | Vulnerability assessment | C | 5 | 0 | 8 | 13 |
| | Control identification | C | 4 | 0 | 8 | 12 |
| | Control assessment | C | 0 | 0 | 6 | 6 |
| | Outcome identification | C | 8 | 8 | 8 | 24 |
| Risk Estimation | | | | | | |
| | Impact Area Prioritization | OA | 4 | 8 | 3 | 15 |
| | Threat motivation | C | 0 | 6 | 7 | 13 |
| | Threat Capability | C | 0 | 0 | 7 | 7 |
| | Threat Capacity | C | 0 | 0 | 7 | 7 |
| | Qualitative Consequence Estimation | C | 8 | 8 | 8 | 24 |
| | Qualitative Probability Estimation | C | 7 | 7 | 8 | 22 |
| | Risk Scenarios | C | 8 | 8 | 8 | 24 |
| | Risk Matrix/table | C | 7 | 6 | 7 | 20 |
| Risk treatment | | | | | | |
| | Risk Prioritization | C | 7 | 8 | 8 | 23 |
| | Treatment plan | C | 8 | 8 | 8 | 24 |
| | Cost/benefit analysis | OA,ISO | 6 | 8 | 8 | 22 |
| | Residual Risk | ISO | 4 | 4 | 6 | 14 |
| Completeness Score | | | 121 | 148 | 184 | |

Table IV compares each ISRA method's theoretical CURF scores to the observed results in the delivered risk reports. The content of the table was constructed from the observable contents of the reports and supplied with tasks from CURF, in total seventy-eight comparisons. The analysis assumes that a successful prediction includes both addressed and partially addressed tasks for both CURF and the reports, or a double absent. An unsuccessful prediction then constitutes occurrences where a task was present in one but not the other. Basing the analysis on this assumption, CURF predicted sixty-five out of the seventy-eight tasks documented in the reports, including nine double absent. In total, there were twelve unsuccessful predictions regarding tasks present in the reports but not in CURF.

Further, we found that some of the technical tasks from Table I were not included in the reports: Any conducted *Preliminary assessment* was not documented in the reports, nor had any of the groups recorded work with *Business process identification*, *Risk Quantification*, or *Risk aggregation*. The three latter tasks are alternative and advanced approaches which limited their usefulness for the novices in the study and were not necessary for completing the project. Besides these four tasks, no fully *addressed* tasks in CURF were ignored in the reports. The results in Table III shows that having a task adequately addressed in the ISRA method influences the content of the report and vice versa. Some notable examples: we see from the analysis of NSMROS that leaving the threat and control assessment out of the method resulted in them being left out of the report. OA does not include a vulnerability assessment scheme which produced four reports without it. However, there are some exceptions; an unmentioned task in CURF was adequately addressed in the reports in two instances: NSMROS *Stakeholder identification* and OA *Cost/benefit analysis*; These tasks were necessary to complete the risk assessment, for example, all the groups were dependent on interviews for data collection and needed to know the stakeholders to run their projects. Another example was organizational understanding using NSMROS, which does not provide any detail on how to achieve this objective. However, we saw from the reports that all the NSMROS groups had worked with risk criteria and to some degree with understanding organizational business objectives. Another issue with NSMROS was that proposing to conduct the control efficiency assessment after the risk evaluation is completed resulted in none of the NSMROS groups doing it. Thus, the sequence of ISRA tasks also matters for the results.

TABLE IV. COMPARISON OF OBSERVABLE THEORETICAL DIFFERENCES FROM CURF AND DIFFERENCES IN REPORTS. *XX=Addressed, X=Partially addressed, & 0=Not addressed*

| | | NSMROS | | OCTAVE A | | ISO27005 | |
|---|---|---|---|---|---|---|---|
| | Task | CURF | Report | CURF | Report | CURF | Report |
| Case descr. | | | | | | | |
| | Organizational Dr. | 0 | X | XX | XX | 0 | X |
| | Risk Measurement Criteria | X | XX | XX | XX | XX | XX |
| | Org. Goals/ Business objectives | 0 | X | XX | X | XX | XX |
| Risk Identi. | | | | | | | |
| | Stakeholder Id. | 0 | XX | X | XX | XX | XX |
| | Asset Identification | XX | XX | XX | XX | XX | XX |
| | Asset Evaluation | XX | X | X | XX | X | XX |
| | Asset Container | 0 | 0 | XX | XX | 0 | X |
| | Threat Identification | XX | X | XX | XX | XX | XX |
| | Threat Assessment | X | 0 | XX | X | XX | XX |
| | Areas of concern/ Vulnerability Id. | X | XX | X | XX | XX | XX |
| | Vulnerability assessm. | 0 | X | 0 | 0 | XX | XX |
| | Control identification | 0 | X | X | 0 | XX | XX |
| | Control assessment | 0 | 0 | 0 | 0 | XX | XX |
| | Outcome identification | XX | XX | XX | XX | XX | XX |
| Risk Est. | | | | | | | |
| | Impact Area Pri. | 0 | X | XX | XX | 0 | X |
| | Threat motivation | 0 | 0 | XX | XX | XX | XX |
| | Threat Capability | 0 | 0 | 0 | 0 | X | XX |
| | Threat Capacity | 0 | 0 | 0 | 0 | X | XX |
| | Qualitative Conseq. Estimation | XX | XX | XX | XX | XX | XX |
| | Qualitative Prob. Estimation | X | XX | X | XX | XX | XX |
| | Risk Scenarios | XX | XX | XX | XX | XX | XX |
| | Risk Matrix/table | XX | XX | XX | XX | XX | XX |
| Risk Eval. & Treatment | | | | | | | |
| | Risk Prioritization | XX | XX | XX | XX | XX | XX |
| | Treatment plan | XX | XX | XX | XX | XX | XX |
| | Cost/benefit analysis | XX | XX | 0 | XX | X | XX |
| | Residual Risk | X | X | XX | X | XX | XX |
| *Total Results* | *Occurrences* | XX-XX | 40 | XX-X | 5 | X-XX | 11 |
| *(CURF-Rep.)* | *(Total 78)* | X-X | 1 | X-0 | 2 | 0-0 | 9 |
| | | 0-X | 8 | 0-XX | 2 | | |

### B. Experienced differences

The critique we gathered of each method had few overlaps with the technical differences: We found that all the risk assessment groups preferred templates and examples: the OA groups ranked the worksheets as most helpful, and the other groups actively looked for templates and examples in other sources. However, one of the drawbacks of the OA worksheets was the amount of paperwork and extra overhead they created. Both the ISO27005 and OA groups sought out mother tongue sources to compensate for the technical non-native language, indicating that technical language was a hindrance for usability. Another practical difference was that the NSMROS groups primarily looked for templates and examples on how to conduct ISRA, together with information on how to scope the assessment.

OA also introduces the identification of organizational drivers as a task. However, all groups struggled with defining the drivers and separating them from organizational vision, mission, goals and key performance indicators. Although understanding the organization is highlighted in both OA and ISO27005, our results indicate that the guidelines are not sufficiently substantiated for novices.

ISO27005 came out best in CURF and was clearly stronger in practice when it comes to threat, vulnerability, and control assessments. All the delivered ISO27005 reports were consistently better at describing these areas, and the groups were satisfied with the descriptions of these areas. However, some of the other issues encountered by all the groups were already known in the academic literature [7], [11], such as difficulties with PxC estimations, organizational alignment, and asset evaluation. Our results show that these tasks are still difficult even when described well in the methodology. In particular, the lack of probability calculations in OA created practical problems for all the groups, due to not being able to prioritize risks with the same consequence and distinct difference in the rate of occurrence.

To summarize, user-friendliness was primarily what the groups cared about, including templates, understandable language, and how-to descriptions. There were observable differences between the work processes of applying each method, and several of these differences are also documented in Table III. Our study also found common issues to all ISRA methods, especially related to data collection, information gathering, and analysis. Such as knowing what data to collect, analysis of interviews, and response rates on questionnaires. Furthermore, all groups struggled with general stakeholder management, such as scheduling interviews, knowing who to interview, various communication issues, and discovering credible sources beyond the interviews.

## VI. Conclusion

Our results show that the choice of ISRA method does matter both regarding content, experience, and produced results. Our novel application of CURF to analyze metadata worked well to establish a cause-effect relationship between ISRA tasks and results. Besides, we found a clear relationship between method and report completeness, whereas the ISO27005 groups scored highest. When inexperienced risk assessors apply a method, its content matters strongly for both the ISRA process and outcome. A lot of the feedback on the use of methods was related to user-friendliness and not related to process or tasks. However, Some issues are universal and should be prepared for, such as data collection issues with analysis and stakeholder management. Besides, the necessity of some tasks for succeeding forced the practitioners to conduct them whether they were present in the framework or not. The participating groups also favored easy to learn methods with checklists and examples, which are desirable items to include into ISRA methods. Our results should strengthen the research incentive within specific ISRA areas, in particular, method development and usability, tools for organizational understanding, and ISRA application and comparison.

### A. Limitations & Future Work

One limitation of this study was that we had different case studies for each group, which limited our ability to isolate the method variable regarding ISRA results. Another limitation of our data is that they were gathered from novices and may not apply for specialists and experts. However, we know from experience that on-site personnel and non-specialists often conduct ISRA, for whom, the method is essential, and our results do apply. Using students has its limitations; first, they have diverse interest and ability, which determines the quality of the result. Secondly, most of the groups needed guidance to complete the assignment, which may lead to supervisors influencing the results. The sample size is an issue in resource intensive qualitative studies; although the results were strongly indicative, four reports per method may not be enough evidence to conclude. Another limitation was that we had a delay for experience data collection with the NSMROS groups, which caused fewer participants to share their experiences.

Data collection is crucial for the ISRA, and a path for future research is studies of data collection methods and techniques for making the ISRA more efficient. Since CURF still is an innovative approach and not fully developed, further development and expansion of CURF is also possible. We showed in the report assessments that the model is adaptable. However, the idea of CURF can be applied for other comparisons and expanded further by adding more nodes in the tree, for example, expanding with the issues uncovered through practical experience. Lastly, we encourage others to conduct similar studies and these will benefit the ISRA community by determining what works and what does not.

## Acknowledgments

The author thanks Christoffer V. Hallstensen, Nils Kalstad Svendsen, Stian Husemoen, Ole Ingvart Langfeldt, NTNU IT, Einar Snekkenes, the anonymous reviewers, Sarah Louise Bergdølmo, Dimitra Anastasopoulou, and the A-IMT1132 students from 2010-2016.

## REFERENCES

[1] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (isra)," *Computers & Security*, vol. 57, pp. 14–30, 2016.

[2] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," DTIC Document, Tech. Rep., 2007.

[3] *Information technology, Security techniques, Information Security Risk Management*, International Organization for Standardization Std., ISO/IEC 27005:2011.

[4] NSM, "Veiledning i risiko- og srbarhetsanalyse (guidelines for risk and vulnerability assessments)," Nasjonal Sikkerhetsmyndighet (Norwegian National Security Authority), Tech. Rep., 2006.

[5] G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness - core unified risk framework," in *Submitted Manuscript*. .., 2015.

[6] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (isra)," *Journal of Information Security and Applications*, vol. 18, no. 1, pp. 45–52, 2013.

[7] G. Wangen and E. Snekkenes, "A taxonomy of challenges in information security risk management," in *Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse - NISK 2013 - Stavanger*, vol. 2013. Akademika forlag, 2013.

[8] *Information technology, Security techniques, ISMS, Overview and vocabulary*, International Organization for Standardization Norm, ISO/IEC 27000:2014. [Online]. Available: http://dx.doi.org/10.3403/30236519

[9] B. Blakley, E. McDermott, and D. Geer, "Information security is information risk management," in *Proceedings of the 2001 workshop on New security paradigms*. ACM, 2001, pp. 97–104.

[10] P. L. Campbell and J. E. Stamp, *A classification scheme for risk assessment methods*. Sandia National Laboratories, 2004.

[11] G. Wangen, "An initial insight into information security risk assessment practices," in *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems*, ser. Annals of Computer Science and Information Systems, M. Ganzha, L. Maciaszek, and M. Paprzycki, Eds., vol. 8. IEEE, 2016, pp. 999–1008. [Online]. Available: http://dx.doi.org/10.15439/2016F158